



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,802	01/09/2004	Hoe-Won Kim	678-1131	1597
66547	7590	04/11/2008		
THE FARRELL LAW FIRM, P.C. 333 EARLE OVINGTON BOULEVARD SUITE 701 UNIONDALE, NY 11553			EXAMINER	
		PALIWAL, YOCESH		
		ART UNIT	PAPER NUMBER	
		2135		
		MAIL DATE		DELIVERY MODE
		04/11/2008		PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Continuation of 11: The request of reconsideration has been considered but does NOT place the application in condition for allowance because: applicant's arguments filed 3/19/2008 have been fully considered but are not persuasive for following reasons:

- Applicant argues that: "The present invention provides improvements in data security over prior art such as Akiyama because, as described above, the cipher key K_s used to encipher the data M requested by a communication terminal can only be obtained by decoding the personal secret key $\{K_s\}K_h$ generated in accordance with an enciphering operation of the K_s enciphering unit, by using the hidden secret key K_h intrinsically assigned to the communication terminal. Accordingly, although enciphered data is circulated over public networks, its original data can be secured."
- Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.
- Applicant further argues that: "More particularly, the Examiner has failed to establish a *prima facie* case of anticipation based on Akiyama because Akiyama fails to disclose a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (K_h) corresponding to intrinsic identification information; a first decoding unit for receiving via a public network a personal secret key ($\{K_s\}K_h$), generated by enciphering a cipher key (K_s) by using the hidden secret key (K_h), and decoding the personal secret key ($\{K_s\} K_h$) by using the hidden secret key thereby obtaining the cipher key (K_s); and a second decoding unit for receiving via the public network enciphered data ($\{M\} K_s$), generated by enciphering data (M) by using the cipher key (K_s), and decoding the enciphered data

({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M), as recited in independent Claim 1 and similarly recited in independent Claims 3, 6, 7 and 10."

➤ Examiner disagrees and still maintain that Akiyama discloses:

a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information (Fig. 14, Numeral 505, "Master Key Storage Unit (Km)");
a first decoding unit for receiving via a public network a personal secret key ([Ks]Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (Paragraph 0108, "The reception device provided at each user's home receives the encrypted appending information ([Appending] Km) and decrypt it using the master key Km provided in that reception device", Note: appending information contains a channel key Kch) and

a second decoding unit for receiving via the public network enciphered data ([M]Ks), generated by enciphering data (M) by using the cipher key (Ks) (Paragraph 0107, The broadcast station 200 broadcasts contents information ([Contents] Kch) which is encrypted using a channel key Kch"), and

decoding the enciphered data ([M]Ks) by using the cipher key (Ks), thereby obtaining the data (M) (Paragraph 0108, "...Channel key Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents] Kch)").

Accordingly, examiner maintains that independent claims 1, 3, 6, 7 and 10 are completely anticipated by Akiyama and are not in condition of allowance. For at least the above reasons, it is believed that the rejection is maintained.

/Y. P./

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135